AIR WAR COLLEGE

AIR UNIVERSITY

CYBERSPACE OPERATIONS, STUXNET, *JUS AD BELLUM* AND *JUS IN BELLO*

by

Grady O. Morton, Jr., Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Howard M. Hensel

14 February 2013

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Grady O. “Jed” Morton is a United States Air Force Reserve Judge Advocate attending the Air War College, Air University, Maxwell AFB, AL. He graduated from the U.S. Air Force Academy in 1988 with a Bachelor of Science degree in Applied Mathematics and earned a Juris Doctor, *magna cum laude*, from the Georgia State University College of Law in Atlanta. He previously served for twelve years as a fighter pilot, instructor pilot, and mission commander in the F-16, and is a combat veteran of Iraq and Afghanistan. In his civilian capacity, Lieutenant Colonel Morton is an Atlanta-based Boeing 777 pilot for Delta Air Lines, Inc.

Abstract

Air Force Doctrine Document 3-12 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Cyberspace attacks are on the rise. In September 2012, hackers attacked Canadian energy companies that manage 60 percent of all oil and gas pipelines in North and Latin America. At about the same time, sophisticated hackers attacked several large United States banking institutions in cyberspace attacks that experts concluded had been planned for weeks. And the now-famous Stuxnet "cyber weapon" infected the software that controls Iran's nuclear weapons centrifuges, resulting in what some experts believe was the first cyberspace attack targeting infrastructure control software.

This paper will analyze the application of the law of armed conflict to cyber operations, applying *jus ad bellum* principles to cyber operations in order to determine when a cyberspace "attack" constitutes a use of force. Then, applying the *jus ad bellum* principles to the Stuxnet worm, the paper argues that Stuxnet constituted a use of force under Article 2(4) of the United Nations Charter. Further, analyzing the *jus in bello* principles of proportionality, military necessity, and discrimination, the paper concludes that the Stuxnet attack complied with all applicable principles of international humanitarian law.

Introduction

> *"If we detect an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us, to defend this nation when directed by the president. For these kinds of scenarios, the department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace."*
>
> Secretary Of Defense Leon E. Panetta, Intrepid Sea, Air & Space Museum, 11 Oct 2012

Air Force Doctrine Document 3-12, *Cyberspace Operations*, is the Air Force's foundational doctrine publication for cyberspace operations. National cyberspace doctrine reflects a primary emphasis on defensive cyberspace operations—securing our own cyber infrastructure from attack and exploitation by hostile forces. National cyberspace doctrine, however, also specifically contemplate offensive cyberspace operations across the range of military operations. AFDD 3-12 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] And while there is no internationally accepted definition of "cyber warfare," the International Committee of the Red Cross defines it as "any hostile measures against an enemy designed to discover, alter, destroy, disrupt, or transfer data stored in a computer, manipulated by a computer or transmitted through a computer."

Incidents of "cyber warfare," within the meaning of the ICRC definition, are on the rise. In September 2012, hackers attacked Canadian energy companies that manage 60 percent of all oil and gas pipelines in North and Latin America.[2] At about the same time, sophisticated hackers attacked several large United States banking institutions in cyberspace attacks that experts

concluded had been planned for weeks.[3] And the now-famous Stuxnet "cyber weapon" infected the software that controls Iran's nuclear weapons centrifuges.

This paper will analyze the application of the law of armed conflict to cyber operations. First, I will apply *jus ad bellum* principles to cyber operations in order to determine when a cyberspace "attack" would constitute a use of force. I will then discuss *jus in bello* principles as applicable to a cyberspace operation which, like Stuxnet, rises to the level of a use of force. I will apply the derived frameworks to the Stuxnet cyberspace operation, which many experts believe was the first cyberspace attack targeting infrastructure control software. My goal is to provide cyberspace warriors and their legal counsel with a road map through the legal maze of conducting military cyberspace operations in compliance with the strictures of relevant international law.

Jus ad bellum

Plato quipped that, "Only the dead have seen the end of war." Indeed, human conflict is as old as humankind. Early in our history, no justification for war was needed other than mankind's desire to satisfy his lust to rape, pillage, and murder.[4] But as humans evolved and carnal impulses gave way to reason, man increasingly sought to justify waging war. By the early twentieth century, mankind's collective conscience had evolved to an established norm that war required justification. Even the pretexts that were used to initiate World War I, and to some extent World War II, evidenced a collective realization that war required justification and should not be entered into absent a "just cause."[5]

Thus, *jus ad bellum* is the law of conflict management—the codification of mankind's collective realization that a moral requirement exists to justify war. *Jus ad bellum* is a set of rules designed to govern when states may resort to armed conflict and to retrospectively determine

whether an armed conflict was lawful or unlawful in its inception. Central to the concept of *jus ad bellum* is the idea of what constitutes a "use of force" by one entity against another. Whether a use of force has occurred is relevant to determining when a state of war exists between states, and whether a state may legitimately invoke its inherent right of self-defense and engage in a use of force against another state.

Article 2(4) of the Charter of the United Nations is the contemporary legal framework for *jus ad bellum*. It applies as positive law to all member nations, and it is considered customary international law, thus making it applicable even to non-signatory nations. Article 2(4) requires states to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state…."[6] According to Walter Gary Sharp, Sr., Articles 2(4), 39, and 51 of the United Nations Charter now redefine and codify the contemporary *jus ad bellum* in its entirety. [7] Sharp further points out that, "If a state activity is a use of force within the meaning of Article 2(4), it is unlawful unless it is an exercise of that state's inherent right of self-defense or unless it is authorized by the Security Council under its coercive Chapter VII authority."[8]

Article 39 is the source of the United Nations' coercive power: "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."[9] For the purposes of this paper, I will assume no explicit Article 39 authorization exists for a use of force in cyberspace. Thus, the only permissible use of force, for the purposes of this paper, would be a state invoking its inherent right of self-defense under Article 51.

Article 51 provides as follows:

> Nothing in the present Charter shall impair the inherent right or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Several frameworks have been advanced in an effort to define what constitutes a cyber "use of force" within the meaning of Article 2(4). One of the more robust frameworks was developed in 1999 by Professor Michael Schmitt. The "Schmitt Analysis" contains seven criteria to be used to evaluate whether a given cyber operation would rise to the level of a prohibited use of force: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[10]

Using the Schmitt criteria, Lt Col Andrew C. Foltz in 2012 argued that the Stuxnet virus constituted a use of force against Iran.[11] Foltz further argued that, if a state-sponsored cyber operation were deemed a use of force, it "could trigger [the target state's] right to self-defense and thereby permit a forceful, perhaps even armed response."[12] By making this argument, Foltz necessarily equated Article 2(4)'s "use of force" with Article 51's "armed attack," since Article 51 does not employ the term "use of force," but instead permits a state to invoke its inherent right to self-defense only after it has been the target of an "armed attack."

The question whether Article 2(4)'s use of force equates to Article 51's armed attack is an important open question among international law scholars.[13] Some argue that the clear implication of the use of different terminology means that there must be a "gap" between a use of force under Article 2(4) and an "armed attack" under Article 51.[14] Others argue that no such gap exists in cyberspace.[15] The most obvious implication of the latter argument is that the same

act by an aggressor state that would constitute a violation of Article 2(4) as an unlawful use of force would simultaneously trigger the target state's inherent right of self-defense under Article 51. Proponents of the "gap view" have not explained what recourse a target state would have, should an act by an aggressor state be deemed an illegal use of force under Article 2(4), yet short of an armed attack under Article 51. Indeed, such a scenario, in which a target state would be left legally defenseless except for recourse to the international justice system, seems absurd. The absurdity of this result militates in favor of an Article 2(4) "use of force" being equated with an Article 51 "armed attack." Indeed, a United States government lawyer attending a 2012 Naval Academy conference on military cyber operations concluded that the United States has taken this as its official position on the issue.[16] Therefore, for the purposes of this paper, the term "use of force" will carry the same meaning as an "armed attack" under Article 51.

With respect to the seven criteria advanced by Professor Schmitt to determine the threshold of what constitutes a cyberspace use of force, battlefield commanders and their legal advisers, operating under the constraints of time and the stress of battle, would be better-served by a simpler model.[17] In this regard, I propose replacing the Schmitt criteria with a relatively straightforward two-pronged definition that combines the element of intent with Schmitt's invasiveness criteria. Thus, for the purposes of this paper, a cyberspace use of force is any cyberspace operation which (1) is intended to cause physical damage to property or death or injury to persons; and (2) which involves a physical invasion of the sovereignty of the target nation's cyberspace infrastructure. Any cyberspace operation that meets these two criteria will be considered both a use of force under Article 2(4) and an armed attack under Article 51.

Stuxnet

According to the New York Times, early in his administration, President Barack Obama secretly ordered a series of sophisticated attacks on Iran's uranium enrichment facility at Natanz.[18] The result of the attack in Iran has been widely reported: it destroyed approximately 1,000 of the 9,000 centrifuges that were being used to enrich uranium at Iran's Natanz facility.[19]

Even though the effect—destruction of physical assets—was the same as any kinetic weapon, Stuxnet was a computer worm, which PC Magazine defines as "a destructive program that replicates itself throughout a single computer or across a network, both wired and wireless."[20] The difference between a computer virus and a computer worm is that the term "worm" implies an automatic method for self-reproduction in other computers.[21] Stuxnet was spread via the Microsoft Windows operating system to over 60,000 computers in Iran, India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland, and Germany.[22] After it was initially introduced, Stuxnet continued to spread until the occurrence of its built-in expiration date of 24 Jun 2012.[23]

Stuxnet was programmed to target only specific Siemens programmable logic controllers (PLCs)—those that controlled the Natanz centrifuges' frequency converter drives.[24] It worked by reprogramming the PLCs, which caused varying amounts of power to be supplied to the motors that turned the centrifuges. Thus, instead of being kept at the constant high speed required to separate and concentrate Uranium-235 for use in reactors and nuclear weapons, the now-reprogrammed PLCs varied the amount of electrical current delivered to the centrifuges, which caused them to switch back and forth between high and low speeds. Ultimately this oscillation between high and low speeds destroyed the affected centrifuges, thus damaging Iran's nuclear weapons program.

Stuxnet Analysis under *jus ad bellum*

The first step a commander and his legal advisor should take in contemplating a cyberspace operation like Stuxnet is to conduct an analysis to determine whether the operation will objectively be deemed a "use of force" within the meaning of Article 2(4) of the United Nations Charter. Using the Schmitt framework, Lt Col Fultz concluded that Stuxnet was a use of force.[25] With regard to Schmitt's severity criterion, Fultz concluded that Stuxnet was a "per se use of force because it caused physical damage."[26] But to label Stuxnet as a per se use of force simply because it caused damage seems to be an oversimplification of the Schmitt severity criterion.

Applying instead the simplified definition of a "use of force" proffered above, the commander should consider the intent of the operation, combined with the amount of damage actually caused, to determine whether the operation will be a use of force, within the meaning of international conflict management law. In the case of Stuxnet, the intent of its author(s) seems clear: to disrupt the Iranian nuclear program. In other words, the clear intent of the operation was to cause damage to physical infrastructure. Furthermore, infecting the target computers with the worm required the unwitting assistance of Iranian scientists, who inserted infected thumb drives into computers that were "air-gapped," or not connected to the internet. Clearly such actions constituted a physical invasion of Iran's sovereignty. Thus, under this simple definition, Stuxnet constituted a use of force under Article 2(4).[27]

One critical difference between the definition proffered here and the Schmitt analysis is that, here, Stuxnet would have been classified as a use of force, even if no damage had occurred to any of the Natanz centrifuges. Even if no actual damage occurred, the intent to cause damage existed. Furthermore, Iran's national sovereignty was clearly violated by a physical penetration

of its cyberspace infrastructure. Together, these are sufficient to rise to the level of a use of force, even if the mission had been a failure and no damage had occurred.

By way of analogy to a situation where no actual damage is caused, there is little doubt that, if an Iranian ship in international waters just off New York City fired a cruise missile at the Empire State Building, that act would be considered a use of force regardless whether the missile destroyed its intended target or went awry and fell harmlessly into the Long Island Sound. Thus, the Schmitt test ignores the non-results based aspects of a traditional use of force, and in that regard it is deficient. Not only is the definition proffered here simpler and easier to use in the heat of battle, but it also preserves a critical, non-effects based component of a traditional use of force.

Jus in bello

Jus in bello, or international humanitarian law, is a set of rules that govern the conduct of hostilities after they begin. International humanitarian law is independent from the body of law that seeks to provide moral and legal justifications for going to war in the first place—*jus ad bellum*. In contrast, *jus in bello* is designed primarily to limit the suffering caused during war.[28] *Jus in bello* principles are codified in the Hague Convention on the Laws and Customs of War of 1907 and the Geneva Conventions of 1949.[29] The United States is a party to both treaties.[30]

The major tenets of *jus in bello* are distinction, military necessity, and proportionality; the three must be interpreted and applied together in order to achieve the primary goal of protecting innocents from the harmful effects of war. The principle of distinction "obliges belligerent parties to distinguish at all times between civilian persons and objects on the one hand, and combatants and military objectives on the other."[31] The principle of military necessity is

explicitly codified in Article 23, paragraph (g) of the Annex to Hague IV, and forbids the destruction of the enemy's property "unless such destruction or seizure be imperatively demanded by the necessities of war."[32] Finally, the principle of proportionality generally requires belligerents to ensure that collateral damage to civilians is not out of proportion to the military advantage anticipated by that attack.[33] It is undisputed that the principles of *jus in bello* apply to cyber warfare operations conducted during armed conflict.[34]

Distinction

The principle of distinction[35] requires that belligerents distinguish between combatants and noncombatants. The Commander's Handbook elucidates the principle as two interrelated duties. First, commanders must distinguish their forces from the civilian population. Second, commanders must distinguish valid military objectives from civilians or civilian objects before attacking.[36] Furthermore, Article 57.1 of the Protocol Additional to the Geneva Conventions of 12 August 1949 imposes specific requirements on "those who plan or decide upon an attack." For the purposes of this paper, I will refer to such persons as "commanders." First, commanders must "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects…."[37] Second, commanders must "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[38] Third, commanders must not launch any attack "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[39]

There are at least two ways to interpret these requirements in the context of cyber operations. First, Professor Michael Schmitt argues that the analysis must be effects-based.[40]

Schmitt argues that, "it is not the violence of the act that constitutes the condition precedent to limiting the occurrence of an attack, but the violence of the ensuing result."[41] Alternatively, Dr. Knut Dormann of the Legal Division of the International Committee of the Red Cross, argues for an analysis based on the definition of military objectives in Article 52.2 of Additional Protocol I: "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[42] A third possible approach—one suggested by Professor Schmitt—is to consider data resident in computers as "objects," within the meaning of any articulation of International Humanitarian Law, thereby rendering unlawful any operation targeting data being stored on civilian computer systems.[43] Schmitt goes on to opine that this approach would be overly broad.[44]

Applying the principle of distinction to Stuxnet, clearly the ultimate targets of the operation were the uranium-enriching centrifuges. Assuming the centrifuges were in fact enriching uranium for use in nuclear weapons, then the centrifuges themselves were valid military targets. But as one moves farther away from the intended target in the cyberspace world, the chances increase that the venues through which a virus must necessarily pass en route to its ultimate target will be civilian and not military. The best approach, then, is to consider the entire network of computers and interfaces that ultimately control the infrastructure of a targeted military industrial complex as one system. This would eliminate Professor Schmitt's concerns about targeting data stored on civilian computer systems, if those systems were part of a larger industrial complex that had a predominantly military function.

But Stuxnet infected tens of thousands of computers in at least eleven different countries outside Iran. And even though the worm did not cause damage in the majority of those computers, the question arises whether these computers should be considered as having been damaged merely because they were infected with a virus that required the time and effort of technicians to detect and remove. The threshold problem is to determine whether a use of force, within the meaning of Article 2(4), was initiated against these countries. A use of force, as defined above, is any cyberspace operation which (1) is intended to cause physical damage to property or death or injury to persons; and (2) which involves a physical invasion of the sovereignty of the target nation's cyberspace infrastructure. Here, the Stuxnet virus was written with safeguards that rendered it harmless against computers not running the targeted Siemens software. Furthermore, the programmers ensured that the worm would self-destruct in June 2012. Thus, not only was there a lack of intent to cause damage, but there was obvious intent, and great programming effort made, to avoid damage to non-targeted systems. Thus, in spite of the fact that Stuxnet was not confined to the target systems in Iran and infected tens of thousands of other computers around the world, the principle of distinction was observed because there was no intent to damage computers outside Iran. One caveat to the intent-base rule, however, is that a reckless release of a virus—one in which there was no specific intent to damage other computers, but where a substantial certainty of damaging non-targeted systems existed—might lead to liability for a violation of the principle of discrimination in spite of a lack of specific intent to do so.

Military necessity

The principle of military necessity "prohibits the use of any kind or degree of force not required for the partial or complete submission of the enemy with a minimum expenditure of

time, life, and physical resources."[45] Furthermore, in applying this principle, "a commander should ask whether the object of an attack is a valid military objective and, if so, whether the total or partial destruction, capture, or neutralization of the object…will constitute a definite military advantage under the circumstances at the time of the attack."[46] Simply put, the principle of military necessity requires a commander to consider the quantity of force to be expended against a target, and then expend no more force than the amount necessary to achieve the partial or complete submission of the enemy. It is thus a rather quantitative analysis.[47]

In determining whether the Stuxnet cyberspace attack meets the requirement of military necessity, the commander and her legal advisors would need to assess whether the Natanz centrifuges were valid military objectives. To the extent that the centrifuges were believed to be employed in Iran's nuclear weapons development program, as confirmed by open source and intelligence reports, it seems clear that this requirement was met. Furthermore, a cyberspace attack is less force than a kinetic attack, which politicians still insist remains an option to prevent Iran from acquiring nuclear weapons.

Proportionality

The principle of proportionality prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage contemplated."[48] Article 57 of Additional Protocol I further requires commanders to refrain from launching such attacks. Importantly, nothing in the concept of proportionality requires commanders to refrain from causing *any* civilian deaths or injuries to civilian property. It requires only that any civilian deaths or property damage not be excessive in relation to the "concrete and direct military advantage contemplated."

The principle of proportionality forbids an attack that may be expected to cause loss of civilian life or damage to civilian property that would be excessive in relation to the direct military advantage contemplated. In order to analyze proportionality, the direct military advantage must therefore be weighed against the damage to civilian life and property. Here, there was no potential damage to civilian life. But to the extent that Stuxnet potentially infected civilian computers via thumb drives that were inadvertently inserted into them, it arguably caused damage to civilian property. Again, the analysis turns on whether mere infection by a virus, without more, constitutes "damage" to civilian property. Since the virus was programmed to lie dormant on any computer not running the specific Siemens software and then delete itself in June 2012, the infection, in and of itself, cannot constitute "damage." Thus, even though Stuxnet replicated itself on as many as 60,000 computers throughout at least a dozen countries, no damage occurred to systems outside Iran. Therefore, the *jus in bello* requirement of proportionality was met in this case.

Conclusion

Because Stuxnet was the first major cyberspace operation that constituted a use of force under Article 2(4) of the United Nations Charter, it provides a valuable test case for commanders and their legal advisors to apply contemporary rules of conflict management (*jus ad bellum*) and international humanitarian law (*jus in bello*) to a cyberspace operation. This paper offered a simplified framework for determining when a cyberspace operation would constitute a use of force, because a seven-prong test such as the one advanced by Professor Schmitt, while useful in hindsight, would be cumbersome to apply during the heat of battle. Furthermore, my analysis of Stuxnet revealed that, under any framework, the virus constituted a use of force within the

meaning of Article 2(4). Finally, *jus in bello* principles were analyzed, with the conclusion that Stuxnet complied with all relevant provisions of international humanitarian law.

Notes

[1]Air Force Doctrine Document 3.12, 15 Jul 2010, 1.
[2] Nadia Moharib, "Cyber Attackers Hit Canadian Energy Companies," *Toronto Sun*, September 29, 2012, http://www.torontosun.com/2012/09/28/cyber-attackers-hit-canadian-energy-companies.
[3] Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *New York Times*, September 30, 2012, http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html.
[4] Walter Gary Sharp, Sr., *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research Corp. 1999), 27-28.
[5] Howard M. Hensel, ed., *The Prism of Just War* (Burlington, VT: Ashgate Publishing Co., 2010), 10.
[6] U.N. Charter art. 2(4).
[7] Sharp, Cyberspace and the Use of Force, 33.
[8] Ibid.
[9] United Nations Charter, Chapter VII, Art. 39.
[10] See Lt Col Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate" (Air War College Research Report, 2012).
[11] Ibid., 17.
[12] Ibid., 5.
[13] See Duncan Hollis, "Is a Use of Force the Same as an Armed Attack in Cyberspace?" Opinio Juris April 28, 2012, http://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armed-attack-in-cyberspace/.
[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] See, e.g., Col Gary Brown and Maj Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly*, Fall 2012, Endnote 48, 144.
[18] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.
[19] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," February 15, 2011. Institute for Science and International Security, report available at http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/.
[20] Personal Computer Magazine online, PC.com, http://www.pcmag.com/encyclopedia_term/0,2542,t%3Dworm&i%3D54874,00.asp.
[21] Ibid.
[22] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, Vol. 53, February 1, 2011.
[23] Ibid.
[24] Ibid., 24.
[25] Fulz, "Stuxnet," 17.
[26] Ibid.

[27] The question whether Stuxnet was unlawful aggressive use of force under Article 2(4) is being debated by scholars, and is beyond the scope of this paper.
[28] See International Committee of the Red Cross online resources, http://www.icrc.org/eng/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm.
[29] Howard M. Hensel, ed., *The Law of Armed Conflict*, (Burlington, VT: Ashgate Publishing Company, 2007), 26.
[30] Ibid.
[31] Howard M. Hensel, ed., *The Legitimate Use of Military Force*, (Burlington, VT: Ashgate Publishing Company, 2008), 161.
[32] *Air Force Operations and the Law*, (Maxwell AFB, AL: AFJAGS Press, 2009), 20.
[33] Hensel, *Legitimate Use of Military Force*, 189.
[34] See, e.g., Michael N. Schmitt, "Cyber Operations and the *Jus in bello*: Key Issues," Naval War College International Law Studies, March 2, 2011, 3. ("It is incontrovertible that the principle [of distinction] applies to cyber operations conducted during an armed conflict.")
[35] Also referred to by some commentators as, "discrimination." See, e.g., Thomas C. Wingfield, *The Law of Information Conflict* (Falls Church, VA: Aegis Research Corp., 2000), 140.
[36] *The Commander's Handbook on the Law of Naval Operations*, ed. July 2007, Sec. 5.3.2., p. 5.3. [hereinafter the "Commander's Handbook"]
[37] Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3. [hereinafter AP1]
[38] Ibid.
[39] Ibid.
[40] Schmitt, "Cyber Operations and the *Jus in bello*," 6.
[41] Ibid.
[42] Ibid, p. 7. See also AP 1, Art. 52.2.
[43] Schmitt, "Cyber Operations and the *Jus in bello*," 8.
[44] Ibid.
[45] Commander's Handbook, Para. 5.3.1.
[46] Ibid.
[47] Wingfield, *Law of Information Conflict*, 150.
[48] Geneva Conventions Additional Protocol, Art. 51, para. b.

Bibliography

Air Force Doctrine Document 3.12, 15 Jul 2010, 1.

Air Force Operations and the Law. Maxwell AFB, AL: AFJAGS Press, 2009.

Albright, David, Brannan, Paul, and Walrond, Christina. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," February 15, 2011. Institute for Science and International Security, report available at http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/.

Brown, Col Gary and Poellet, Maj Keira. "The Customary International Law of Cyberspace," *Strategic Studies Quarterly*, Fall 2012.

The Commander's Handbook on the Law of Naval Operations, ed. July 2007.

Farwell, James P. Farwell and Rohozinski, Rafal. "Stuxnet and the Future of Cyber War." *Survival*, Vol. 53, February 1, 2011.

Foltz, Lt Col Andrew C. "Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate". Air War College Research Report, 2012.

Hensel, Howard M., ed. *The Law of Armed Conflict*. Burlington, VT: Ashgate Publishing Company, 2007.

Hensel, Howard M. Hensel, ed. *The Legitimate Use of Military Force*. Burlington, VT: Ashgate Publishing Company, 2008.

Hensel, Howard M. ed. *The Prism of Just War*. Burlington, VT: Ashgate Publishing Co., 2010.

Hollis, Duncan. "Is a Use of Force the Same as an Armed Attack in Cyberspace?" Opinio Juris April 28, 2012, http://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armed-attack-in-cyberspace/.

International Committee of the Red Cross online resources, http://www.icrc.org/eng/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm.

Moharib, Nadia. "Cyber Attackers Hit Canadian Energy Companies," *Toronto Sun*, September 29, 2012, http://www.torontosun.com/2012/09/28/cyber-attackers-hit-canadian-energy-companies.

Perlroth, Nicole. "Attacks on 6 Banks Frustrate Customers," *New York Times*, September 30, 2012, http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html.

Personal Computer Magazine online, PC.com, http://www.pcmag.com/encyclopedia_term/0,2542,t%3Dworm&i%3D54874,00.asp.

Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

Schmitt, Michael N. "Cyber Operations and the *Jus in bello*: Key Issues." Naval War College International Law Studies, March 2, 2011.

Sharp, Walter Gary Sr. *Cyberspace and the Use of Force*. Falls Church, VA: Aegis Research Corp. 1999.

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, available at: http://www.unhcr.org/refworld/docid/3ae6b3930.html.
Wingfield, Thomas C. *The Law of Information Conflict*. Falls Church, VA: Aegis Research Corp., 2000.